



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/092,277	03/06/2002	Ian Curry	10500.02.0123	7718

23418 7590 09/20/2007
VEDDER PRICE KAUFMAN & KAMMHOLZ
222 N. LASALLE STREET
CHICAGO, IL 60601

EXAMINER

PICH, PONNOREAY

ART UNIT	PAPER NUMBER
----------	--------------

2135

MAIL DATE	DELIVERY MODE
-----------	---------------

09/20/2007

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

**Advisory Action
Before the Filing of an Appeal Brief**

Application No.

10/092,277

Applicant(s)

CURRY, IAN

Examiner

Ponnoreay Pich

Art Unit

2135

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 11 September 2007 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☒ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:

- a) ☒ The period for reply expires 3 months from the mailing date of the final rejection.
b) ☐ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☐ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because
(a) ☐ They raise new issues that would require further consideration and/or search (see NOTE below);
(b) ☐ They raise the issue of new matter (see NOTE below);
(c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
(d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).

4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. ☐ Applicant's reply has overcome the following rejection(s): _____.
6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
7. ☒ For purposes of appeal, the proposed amendment(s): a) ☐ will not be entered, or b) ☒ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.
The status of the claim(s) is (or will be) as follows:
Claim(s) allowed: _____.
Claim(s) objected to: _____.
Claim(s) rejected: 1-28.
Claim(s) withdrawn from consideration: _____.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing of good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because:
See attached.
12. ☐ Note the attached Information Disclosure Statement(s). (PTO/SB/08) Paper No(s). _____.
13. ☐ Other: _____.

Response to Amendments and Arguments

Applicant's amendments after final rejection are entered as they do not materially affect the scope of the claims and only serve to overcome minor objections.

Applicant argues for the independent claims that Perlman does not teach receiving an encrypted secret key encrypted using a public key associated with a secure distribution server. Applicant states that public key 107 cited in the office action is a group public key and is independent of the DLE 110 and group server 114, thus the limitation under contention is not taught. The examiner respectfully disagrees. Key 107 is called a "group public key" because it is associated with group server 114. In column 5, lines 28-31, Perlman discusses how group public key 107 is used by a sender to encrypt message key 210 before transmission of the message key. In column 5, lines 52-55, Perlman discusses how the group private key 302 is utilized to decrypt the encrypted message key which was encrypted using public key 107. Clearly, public key 107 and private key 302 are asymmetric key pairs. Since private key 302 is stored in group server 114, it is associated with group server 114 and since public key 107 is the reciprocal of key 302, public key 107 is also associated with group server 114. In asymmetric key systems, the owner of a public/private key pair keeps secret the private key while distributing the public key. Since group server 114 owns private key 302, one should appreciate that public key 107 is also owned by and associated with group server 114. As such, applicant's argument that group public 107 is independent of the DLE and group server 114 is incorrect.

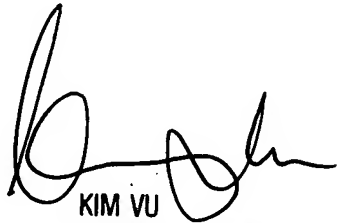
Applicant's arguments for the limitations recited in claims 4-5 appear to be dependent on the assumption that the group public key 107 disclosed by Perlman is not associated with the secure distribution server, i.e. DLE 110 and group server 114. As discussed in the traversal for claim 1, this assumption is incorrect, thus the traversal for claims 4-5 flow from the traversal of claim 1.

As per claim 9, applicant argues that the teachings of Perlman would not allow the forwarding and routing of packets in the nodes of the network to take effect as alleged in the office action since Perlman teaches not to send the encrypted message to the group server. Applicant states that the group server only receives the encrypted message key, not the encrypted message also. The examiner respectfully submits that applicant appears to be misinterpreting the examiner's rejection. The examiner is stating that at the time applicant's invention was made, it was well known to route messages through intermediaries before the message arrives at the final destination. Rarely does a message, which is sent from a sender to a receiver, travel directly from a sender to a receiver. Instead, it is usually routed through several switches and repeaters before arriving at the final destination. For example, consider a network having nodes A, B, C, and D, wherein A is connect to B, which is connected to C, which is connected to D. A message sent from node A to node D would have to be routed through nodes B and C if there was no direct route from A to D. In routing the message from A to D, nodes B and C would typically not perform any sort of decryption on the message as their role in the transaction would only be to forward the message to its final destination, i.e. node D. In the context of Perlman's invention, the sending of the

Art Unit: 2135

encrypted message and encrypted message key from a sender to a receiver reads on the limitation recited in claim 9 in light of it being well known that messages sent from a source to destination usually has to be routed through intermediary nodes before arriving at the final destination.

The argument for claims 11, 14, and 27 is dependent on claim 1 being allowed. However, because claim 1's arguments were traversed, these claims are also not allowable.



KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100